

On the Secure Degrees of Freedom of the K-user MAC and 2-user Interference Channels

Mohamed Amir¹, Tamer Khattab¹ and Tarek Elfouly²

¹Electrical Engineering, Qatar University

²Computer Science & Computer Engineering, Qatar University

Email: mohamed.amir@qu.edu.qa, tkhattab@ieee.org, tarekfouly@qu.edu.qa

Abstract—We investigate the secure degrees of freedom (SDoF) of the K -user MIMO multiple access (MAC) and the two user MIMO interference channel. An unknown number of eavesdroppers are trying to decode the messages sent by the transmitters. Each eavesdropper is equipped with a number of antennas less than or equal to a known value N_E . The legitimate transmitters and receivers are assumed to have global channel knowledge. We present the sum SDoF of the two user MIMO interference channel. We derive an upperbound on the sum SDoF of the K -user MAC channel and present an achievable scheme that partially meets the derived upperbound.

I. INTRODUCTION

The noisy wiretap channel was first studied by Wyner [1], in which a legitimate transmitter (Alice) wishes to send a message to a legitimate receiver (Bob), and hide it from an eavesdropper (Eve). Wyner proved that Alice can send positive secure rate to Bob using channel coding. He derived capacity-equivocation region for the degraded wiretap channel. A significant amount of work was carried thereafter to study the information theoretic physical layer security for different network models. The relay assisted wiretap channel was studied in [2]. The secure degrees of freedom (SDoF) region of multiple access (MAC) channel was presented in [3]. The SDoF is the the pre-log of the secrecy capacity region in the high-SNR regime. Using MIMO systems for securing the message was an intuitive extension due to the spatial gain provided by multiple antennas. MIMO wiretap channel secrecy capacity was identified in [4]. Meanwhile, the idea of cooperative jamming was proposed in [5], where some of the users transmit independent and identically distributed (i.i.d.) Gaussian noise towards the eavesdropper to improve the sum secrecy rate of the legitimate parties.

In this paper, we study the K -user MIMO MAC and the two user MIMO interference channel, each with unknown number of eavesdroppers. We assume that the legitimate pair has global channel knowledge. We present the sum SDoF of the two user MIMO interference channel. We derive an upperbound on the the sum SDoF of the K -user MAC channel and present an achievable scheme that partially meets the upperbound depending on the relations between the nodes' number of antennas. We use the following notation, \mathbf{a} for vectors, \mathbf{A} for matrices, \mathbf{A}^\dagger for the hermitian transpose of \mathbf{A} , $[A]^+$ for the

$\max A, 0$ and $\text{Null}(\mathbf{A})$ to define the nullspace of \mathbf{A} , while $\mathbf{a} \mathbf{C} \mathbf{b}$ is used to define the b -combination of a set a

II. SYSTEM MODEL

We consider two communication systems, the K -user MIMO MAC and the two user MIMO interference channel. The K -user MIMO MAC consists of K transmitters, each is equipped with M antennas and one legitimate receiver equipped with N antennas. The two user MIMO interference channel consists of two transmitters and two receivers, each is equipped with M antennas. Both systems are studied in vicinity of an unknown number of passive eavesdroppers. The j th eavesdropper is equipped with $N_{Ej} \leq N_E$ antennas, where N_E is a constant known to all transmitters. Let \mathbf{x}_i denote the $M \times 1$ vector of symbols to be transmitted by transmitter i , where $i \in \{1, 2, \dots, K\}$. We can write the received signal at the j th legitimate receiver at time (sample) k as

$$\mathbf{Y}_j(k) = \sum_{i=1}^q \mathbf{H}_{i,j} \mathbf{V}_i \mathbf{x}_i(k) + \mathbf{n}_j(k), \quad (1)$$

where $i \in \{1, 2, \dots, K\}$, $j = 1$ and $q = K$ for the MAC channel, $i, j \in \{1, 2\}$ and $q = 2$ for the interference channel and the received signal at the j th eavesdropper is

$$\mathbf{Z}_j(k) = \sum_{i=1}^q \mathbf{G}_{i,j}(k) \mathbf{V}_i \mathbf{x}_i(k) + \mathbf{n}_{Ej}(k), \quad (2)$$

where $\mathbf{H}_{i,j}$ is the matrix containing the channel coefficients from transmitter i to the legitimate receiver j , $\mathbf{G}_{i,j}(k)$ is the matrix containing the channel coefficients from transmitter i to the eavesdropper j , \mathbf{V}_i is the precoding unitary matrix (i.e. $\mathbf{V}_i \mathbf{V}_i^\dagger = \mathbf{I}$) at transmitter i , $\mathbf{n}_j(k)$ and $\mathbf{n}_{Ej}(k)$ are the additive white Gaussian noise vectors with zero mean and variance σ^2 at the legitimate receiver and the j th eavesdropper, respectively. We assume that the transmitters have global channel knowledge. We assume that $N_E < M$. We define the $M \times 1$ channel input from legitimate transmitter i as

$$\mathbf{X}_i(k) = \mathbf{V}_i \mathbf{x}_i(k). \quad (3)$$

Each transmitter i intends to send a message W_i over n channel uses (samples) to the legitimate receiver simultaneously while preventing the eavesdroppers from decoding its message. The encoding occurs under a constrained power given by

$$\mathbb{E} \left\{ \text{tr}(\mathbf{X}_i \mathbf{X}_i^\dagger) \right\} \leq P \quad \forall i = 1, \dots, q \quad (4)$$

Expanding the notations over n channel extensions we get $\mathbf{H}_i^n = \{\mathbf{H}_i(1), \mathbf{H}_i(2), \dots, \mathbf{H}_i(n)\}$. Similarly we can define $\mathbf{G}_{i,j}^n, \mathbf{X}_i^n, \mathbf{Y}^n, \mathbf{Z}_j^n$. At each transmitter, the message W_i is uniformly and independently chosen from a set of possible secret messages for transmitter i , $\mathcal{W}_i = \{1, 2, \dots, 2^{nR_i}\}$. The rate for W_i is $R_i \triangleq \frac{1}{n} \log |\mathcal{W}_i|$, where $|\cdot|$ denotes the cardinality of the set. A secure rate tuple (R_1, \dots, R_q) is said to be achievable if for any $\epsilon > 0$ there is an n -length codes such that the legitimate receiver decode the messages reliably, i.e.,

$$\Pr\{(W_1, \dots, \hat{W}_q) \neq (\hat{W}_1, \dots, \hat{W}_q)\} \leq \epsilon \quad (5)$$

and the messages are kept information-theoretically secure against the eavesdroppers, i.e.,

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W_1, \dots, W_q | \mathbf{Z}_j^n) \geq \lim_{n \rightarrow \infty} \frac{1}{n} H(W_1, \dots, W_q) - \epsilon \quad (6)$$

where $H(\cdot)$ is the Entropy function and (6) implies the secrecy for any subset $\mathbb{S} \subset \{1, 2\}$ of messages including individual messages [6]. The sum SDoF is defined as

$$D_s = \lim_{P \rightarrow \infty} \sup \sum_i \frac{R_i}{\frac{1}{2} \log P}, \quad (7)$$

where the supremum is over all achievable secrecy rate tuples (R_1, \dots, R_q) , $D_s = d_1 + \dots + d_q$, and d_i is the secure DoF of transmitter i .

III. K USER MIMO MAC

Theorem 1. *The number of SDoF of the K user MAC channel is upperbound as,*

$$D_s \leq \begin{cases} \min(KM - N_E, N - \frac{N_E}{K}) & \text{if } M < N \\ M - \frac{N_E}{K} & \text{if } N \leq M < N + \frac{N_E}{K} \\ N & \text{if } M \geq N + \frac{N_E}{K} \end{cases} \quad (8)$$

Proof:

The first bound for $D_s \leq KM - N_E$ represent the DoF loss caused by the number of eavesdroppers' antennas on the transmitter side. Without loss of generality, we provide an upperbound for the case of existence of only one eavesdropper with N_E antennas. The SDoF of the single eavesdropper scenario is certainly an upperbound for the multiple eavesdroppers case, as increasing the number of eavesdroppers can only reduce the SDoF of the legitimate users. Accordingly, we omit the eavesdropper subscript for simplicity of notation. Suppose that we can added $|M - N|^+$ antennas to the receiver side that won't decrease the SDoF, the sum rate is upperbounded by the capacity of an equivalent MIMO wiretap channel with $(M_1 + M_2)$ transmit antennas and $\mathbf{H} = [\mathbf{H}_1 \ \mathbf{H}_2]$, $\mathbf{x} = [\mathbf{x}_1 \ \mathbf{x}_2 \dots \mathbf{x}_K]^T$ and precoding matrix \mathbf{V} . The secrecy capacity (C_s) for the MIMO wiretap channel with one eavesdropper and fixed known eavesdropper channel was presented in [4], and is an upperbound for all cases studied in this paper. It is easy to see that if the eavesdropper channel is unknown and time varying the SDoF is also upperbounded by the fixed channel case. The secrecy capacity (C_s) was found to be equal to,

$$\begin{aligned} C_s &= (\mathbf{X}_1, \mathbf{Y}_1) - I(\mathbf{X}_1, \mathbf{Z}) \\ &= \max_{K_x} \log(|(\mathbf{I} + \mathbf{H}_{1,1} K_x \mathbf{H}_{1,1}^\dagger)|) - \log(|(\mathbf{I} + \mathbf{G} K_x \mathbf{G}^\dagger)|) \end{aligned} \quad (9)$$

where K_x is the covariance matrix of the transmitted signal. As $\mathbf{H}_{1,1}^\dagger \mathbf{H}_{1,1}$ and $\mathbf{G}^\dagger \mathbf{G}$ are hermitian, they can be diagonalized as $\mathbf{G}^\dagger \mathbf{G} = \mathbf{U}_G \mathbf{\Lambda}_G \mathbf{U}_G^\dagger$, $\mathbf{H}_{1,1}^\dagger \mathbf{H}_{1,1} = \mathbf{U}_{H_{1,1}} \mathbf{\Lambda}_{H_{1,1}} \mathbf{U}_{H_{1,1}}^\dagger$, where

$\mathbf{U}_G \mathbf{U}_G^\dagger = \mathbf{I}$ and $\mathbf{U}_G \mathbf{U}_G^\dagger = \mathbf{I}$. Without loss of generality, Let $\mathbf{V} = [\mathbf{V}_L \ \mathbf{V}_N]$, where \mathbf{V}_N contains the N_E orthonormal basis of \mathbf{G} , while \mathbf{V}_L contains the $M - N_E$ basis of the orthogonal complement of \mathbf{V}_N , and $K_x = \mathbf{V} \mathbf{\Lambda}_{K_x} \mathbf{V}^\dagger$. Therefore,

$$\begin{aligned} D_s &\leq \lim_{P \rightarrow \infty} \frac{1}{\log P} (\max_{\mathbf{\Lambda}_{K_x}} (\log |\mathbf{I} + \mathbf{U}_{H_{1,1}} \mathbf{\Lambda}_{H_{1,1}} \mathbf{U}_{H_{1,1}}^\dagger \mathbf{V} \mathbf{\Lambda}_{K_x} \mathbf{V}^\dagger| \\ &\quad - \log |\mathbf{I} + \mathbf{U}_G \mathbf{\Lambda}_G \mathbf{U}_G^\dagger \mathbf{V} \mathbf{\Lambda}_{K_x} \mathbf{V}^\dagger|)) \\ &\stackrel{(a)}{\leq} \lim_{P \rightarrow \infty} \frac{1}{\log P} (\max_{\mathbf{\Lambda}_{K_x}} (\log |\mathbf{\Lambda}_{H_{1,1}} \mathbf{\Lambda}_{K_x}| - \log |\mathbf{\Lambda}_G \mathbf{\Lambda}_{K_x}|)) \\ &\stackrel{(b)}{\leq} \lim_{P \rightarrow \infty} \frac{1}{\log P} (\max_{\mathbf{\Lambda}_{K_x}} (\log \prod_{i=1}^{KM} \lambda_{H_{1,1}}^i \lambda_{K_x}^i - \log \prod_{i=1}^{N_E} \lambda_G^i \lambda_{K_x}^i)) \\ &\leq \lim_{P \rightarrow \infty} \frac{1}{\log P} (\max_{\mathbf{\Lambda}_{K_x}} (\sum_{i=1}^{KM} \log \lambda_{H_{1,1}}^i \lambda_{K_x}^i - \sum_{i=1}^{N_E} \log \lambda_G^i \lambda_{K_x}^i)) \\ &\leq KM - N_E \end{aligned} \quad (11)$$

where $\lambda_{K_x}^i$ is the i th diagonal value of $\mathbf{\Lambda}_{K_x}$ and $\lambda_G^i, \lambda_{H_{1,1}}^i$ are defined similarly. (a) is because $\log |\mathbf{I} + \mathbf{A} \mathbf{B}| = \log |\mathbf{I} + \mathbf{B} \mathbf{A}|$ for the above matrices, (b) is because $\lim_{P \rightarrow \infty} \frac{\log |\mathbf{I} + \mathbf{B}|}{\log P} = \lim_{P \rightarrow \infty} \frac{\log |\mathbf{B}|}{\log P}$ for any matrix \mathbf{B} , and because $|\mathbf{A} \mathbf{B}| = |\mathbf{A}| |\mathbf{B}|$ for square matrices, and $|\mathbf{V}_{K_x}|, |\mathbf{V}_{H_{1,1}}|, |\mathbf{U}|$ are independent of P . ■

The second bound $M - \frac{N_E}{K}$ represents the DoF loss of each transmitter due to the number of eavesdroppers antennas available. Let d_e^i be degrees of freedom of the parts of the messages sent by transmitter i , which can be decoded by the eavesdropper. For the receiver to be able to decode the secure messages with inter-message interference and achieve the designated SDoF of each transmitter, the receiver must be able to project the i th secure signal into an interference free space of dimension d_i . On the other hand, the non secure parts of the messages can overlap at the receiver or even does not reach the receiver because the receiver is not interested in decoding them and treated as interference. Let α_i be the number of degrees of freedom of the non secure part of the message i that reaches the receivers while β_i be the number of degrees of freedom of the part that does not reach the receiver. Accordingly, $d_e^i = \alpha_i + \beta_i$ and the number of degrees of freedom of the message i is equal to $(d_i + \alpha_i + \beta_i)$. Since, the receiver is not interested in decoding the non secure parts with sizes $\{\alpha_i; i = 1, 2, \dots, K\}$, and the non secure messages occupy at least $\max(\alpha_j; j = 1, 2, \dots, K)$ DoF, then

$$\sum_{i=0}^K d_i + \max(\alpha_j; j = 1, 2, \dots, K) \leq N \quad (12)$$

while,

$$\beta_i \leq M - N \ \forall \ i = 1, 2, \dots, K \quad (13)$$

Moreover, since the eavesdropper has $N_E < M$ antennas, i.e the DoF of the transmitted messages is larger than N_E then

$$\sum_{i=0}^K d_e^i = N_E \quad (14)$$

The secure DoF is then upperbounded as

$$D_s \leq \text{maximize } \{d_j; j = 1, 2, \dots, K\} \sum_{i=0}^K d_i \quad (15)$$

$$\text{subject to, } \sum_{i=0}^K d_i + \max(\alpha_j; j = 1, 2, \dots, K) \leq N \quad (16)$$

$$\sum_{i=0}^K (\alpha_i + \beta_i) = N_E$$

$$\sum_{i=0}^K \beta_i \leq K(M - N)$$

The sum SDoF is maximized by minimizing $\max(\alpha_i; j = 1, 2, \dots, K)$. Combining the second and third constraint we have

$$\sum_{i=0}^K \alpha_i \geq N_E - K(M - N) \quad (17)$$

and minimizing $\max(\alpha_i; j = 1, 2, \dots, K)$ is achieved by choosing all $\{\alpha_i; j = 1, 2, \dots, K\}$ to be equal, and $\sum_{i=0}^K \alpha_i = N_E - K(M - N)$. Accordingly,

$$\max(\alpha_j; j = 1, 2, \dots, K) \leq \frac{N_E}{K} - (M - N) \quad (18)$$

and,

$$D_s \leq M - \frac{N_E}{K} \quad (19)$$

Similarly, we can prove that for $M \leq N$, the SDoF is upperbounded as,

$$D_s \leq N - \frac{N_E}{K} \quad (20)$$

The Third bound $D_s \leq N$ is the due to limited number of antennas at the receiver which limits the SDoF.

Achievable scheme:

For securing the legitimate messages, the transmitters uses a two-step noise injection by simultaneously sending a jamming signal and using a stochastic encoder as follows,

- 1) The transmitters send a jamming signal with power $P^J = \alpha P$ that guarantees that all eavesdropper have a constant rate ($o(\log P)$) for all legitimate signal power values, where α is a constant controlled the transmitters to adjust the jamming.
- 2) A stochastic encoder is built using random binning. The encoder randomness rate is designed to be larger than of the post-jamming eavesdroppers leakage, hence all eavesdroppers would have zero rate with the code length goes to infinity meeting the secrecy constraints in (6).

The jamming signal transmitted is a N_E vector $\mathbf{r} = [\mathbf{r}_1 \ \mathbf{r}_2 \dots \ \mathbf{r}_K]^T$ with random symbols using $\{\mathbf{V}_1^J, \mathbf{V}_2^J, \dots, \mathbf{V}_K^J\}$ as jamming precoders¹. Hence, the transmitted coded signal can be broken into legitimate signal, \mathbf{s}_i , and jamming signal, \mathbf{r}_i , the precoder, \mathbf{V}_i can be also broken into legitimate

precoder, \mathbf{V}_i^L , and jamming precoder, \mathbf{V}_i^J such that

$$\mathbf{V}_i \mathbf{x}_i = \begin{bmatrix} \mathbf{V}_i^L & \mathbf{V}_i^J \end{bmatrix} \begin{bmatrix} \mathbf{s}_i \\ \mathbf{r}_i \end{bmatrix}, \in \{1, 2, \dots, K\}.$$

Choosing \mathbf{V}^J to be the unitary matrix, the jamming power becomes $P^J = E\{\text{tr}(\mathbf{r}_i \mathbf{r}_i^H)\} = \alpha P$, where α is a constant controlled by the transmitter.

Proposition 1. *The jamming signal, \mathbf{r} , overwhelms all eavesdroppers' signal space, and all eavesdroppers end up decoding zero DoF of the legitimate messages. The transmitter then uses a stochastic encoder to satisfy the secrecy constraint in (6)*

Let $\bar{R}_e = I(\mathbf{Z}; \mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_K)$ be the rate of the eavesdropper with the best channel assuming in worst case scenario that it also has N_E antennas. Let $R_e = I(\mathbf{Z}; \mathbf{W}_1, \mathbf{W}_2, \dots, \mathbf{W}_K)$ be the legitimate message rate of the same eavesdropper, where $R_e < \bar{R}_e$ because of the stochastic encoder used. let \bar{R}_{ej} be the rate of the j th eavesdropper. Then $\bar{R}_{ej} \leq \bar{R}_e \forall j \in L$, where L is the unknown number of eavesdroppers.

Proof:

$$\begin{aligned} n\bar{R}_e &\leq I(\mathbf{Z}^n; \mathbf{s}_1^n, \mathbf{s}_2^n, \dots, \mathbf{s}_K^n) \\ &= h(\mathbf{Z}^n) - h(\mathbf{Z}^n | \mathbf{s}_1^n, \mathbf{s}_2^n, \dots, \mathbf{s}_K^n) \\ \bar{R}_e &= h(\mathbf{Z}) - h(\mathbf{Z} | \mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_K) \\ &\leq N_E \log P - N_E \log P^J + o(\log P) \\ &\leq N_E \log P - N_E \log \alpha P + o(\log P) \\ &\leq o(\log P) = C_E \end{aligned} \quad (21)$$

where C_E is a constant that does not depend on P and known to the transmitters. ■

Remark 1. *The constant eavesdropper post-jamming rate comes from the fact that P^J is controlled by the transmitter. Hence, setting $P^J = \alpha P$, a constant SNR is guaranteed at the eavesdroppers and a constant rate independent of P . For the case of the constant known eavesdropper channel or unknown fading channel with known statistics, the constant C is known transmitter.*

The transmitters use the post-jamming rate difference to transmit perfectly secure messages using a stochastic encoder similar to the one described in [8] according to the strongest eavesdropper's rate, C , in worst case scenario to achieve the secrecy constraint in 6. The Wyner code $C_i \in C(R_i^t, R_i, n) \forall i = 1, 2, \dots, K$ of size $2^{nR_i^t}$ is used to encode a confidential message set $W_i = \{1, 2, \dots, 2^{nR_i}\}$ of transmitter i , R_i^t is the transmitted total rate and R_i the secure message rate (i.e. $R_i^t \geq R_i$), and n is the codeword length. As a result, the rate $R^l = R_i^t - R_i$ is the cost of secrecy or the rate lost to secure the legitimate message. For a Wyner code, if $\bar{R}_e = R_l$, then the eavesdropper cannot decode the secure message sent (i.e. $\lim_{n \rightarrow \infty} \frac{1}{n} R_e \leq \epsilon$). The Wyner code $C(R_i^t, R_i, N)$ is built using random binning [9]. We generate $2^{nR_i^t}$ codewords $s_i^n(w_i, v_i)$, where $w_i = 1, 2, \dots, 2^{nR_i}$, and $v_i = 1, 2, \dots, 2^{n(R_i^t - R_i)}$, by choosing the $2^{nR_i^t}$ symbols $s_i(w_i, v_i)$ independently at random according to the input distribution $p(s_i)$. Then we distribute them randomly into 2^{nR_i} bins such that each bin contains $2^{n(R_i^t - R_i)}$ codewords. The stochastic encoder of $C(R_i^t, R_i, N)$ is described by a

¹For the special case $N_E = 1$, only one user sends a single jamming symbol.

matrix of conditional probabilities so that, given $w_i \in W_i$, we randomly and uniformly select a codeword to transmit from the bin w_i or in other words, we select v_i from $\{1, 2, \dots, 2^{n(R_i - R_i)}\}$ and transmit $s_i^n(w_i, v_i)$. We assume that the legitimate receiver employs a typical-set decoder. Given the received signal y^n , the legitimate receiver tries to find a pair (\hat{w}, \hat{v}) so that $s^n(\hat{w}, \hat{v})$ and y^n are jointly typical [9]. We set $R_i = I(s_i, \mathbf{Y}_1) - I(s_i, \mathbf{Z}) - \epsilon$ and $R_i^t = I(s_i, \mathbf{Y}_1) - \epsilon$. The error probability and equivocation calculations are straight forward extensions of similar Wyner random binning encoders [9],

$$H(\mathbf{W}_i^n) = I(s_i^n; \mathbf{Y}^n) - I(s_i^n; \mathbf{Z}^n) - m\epsilon \quad (22)$$

$$H(\mathbf{W}_i^n | \mathbf{Z}^n) = I(s_i^n; \mathbf{Y}^n | \mathbf{Z}^n) - I(s_i^n; \mathbf{Z}^n | \mathbf{Z}^n) - n\epsilon \quad (23)$$

$$= I(s_i^n; \mathbf{Y}^n, \mathbf{Z}^n) - I(s_i^n, \mathbf{Z}^n) - n\epsilon \quad (24)$$

$$\geq H(\mathbf{W}_i^n) - n\epsilon \quad (25)$$

and,

$$H(\mathbf{W}_1^n, \dots, \mathbf{W}_K^n | \mathbf{Z}^n) = \sum_i^K H(\mathbf{W}_i^n | \mathbf{Z}^n) \quad (26)$$

$$\geq \sum_i^K H(\mathbf{W}_i^n) - Kn\epsilon \quad (27)$$

$$\geq H(\mathbf{W}_1^n, \dots, \mathbf{W}_K^n) - Kn\epsilon \quad (28)$$

. Let \mathbf{U} be the post-processing matrix that projects the signal into a jamming free space at the legitimate receiver. The secure messages sum rate is then,

$$\sum_{i=1}^K R_i \geq \frac{1}{2} \log \left| \mathbf{I} + \sum_{i=1}^K (\mathbf{U} \mathbf{H}_i \mathbf{V}_i^L \mathbf{s}_i \mathbf{s}_i^\dagger \mathbf{V}_i^{L\dagger} \mathbf{H}_i^\dagger \mathbf{U}^\dagger) \right| - R_e \quad (29)$$

As $\lim_{n \rightarrow \infty} \frac{1}{n} R_e \leq \epsilon$ for all values of \mathbf{G}_i and P , a positive secrecy rate, which is monotonically increasing with P , is achieved. Computing the secrecy degrees of freedom boils down to calculating the degrees of freedom for the first term in the right hand side of (29), which represents the receiver DoF after jamming is applied. Next we will calculate the SDoF and show how jamming is designed to Maximize the achievable SDoF.

A. Achievability for $M \geq N + \frac{N_E}{K}$

For this region, the transmitters send the jamming signals using precoders \mathbf{V}_i^J , using *Nullspace jamming*, respectively. All the precoders have $\frac{N_E}{K}$ jamming streams such that the total number of jamming streams reaching each eavesdropper equal N_E .

Nullspace jamming: In nullspace jamming method, the transmitter i sends a jamming signal of J_i dimensions using the precoder \mathbf{V}_i^J which lies in the nullspace of the channel \mathbf{H}_i ,

$$\mathbf{V}_i^J = \text{Null}(\mathbf{H}_i) \quad i \in 1, 2, \dots, K \quad (30)$$

This blocks N_E dimensions at each eavesdropper and leaves N free dimensions at the legitimate receiver to attain the legitimate signal, thus the following sum SDoF is achievable,

$$D_s \leq N \quad (31)$$

B. Achievability for $M < N$

For this region we use *aligned jamming* for blocking the eavesdropper where jamming is aligned at the receiver to minimize the wasted space and maximize the SDoF

Aligned jamming: The jamming signals of both transmitters are aligned at the legitimate receiver signal space. Each group j of transmitters of size $L_j \leq K$ aligns portions of its jamming signal together at the receiver. There are KCL_j groups of size L , while the total number of groups $\sum_{a=2, b \leq a}^{a=K} iC_j$, the number of jamming of streams assigned to each group (J_g/N_E) depends on the relation between (M, N, N_E) . Let \mathcal{I}_j be the jamming space at the receiver designated for group j . Each transmitter aligns a part or the whole of its jamming signal into this jamming space. The total signal space of transmitter i occupies *only* $M < N$ dimensions at the receiver. This make the received signal spaces of different transmitters distinct at the receiver. So a common space is needed to direct the jamming signal into. Let A_i span the received signal space of transmitter i , i.e span the space including all possible received vectors at the receiver, \mathcal{I} is chosen to be the intersection of these spaces, i.e.,

$$\mathcal{I}_j = \bigcap_{i=1}^{L_j} A_i. \quad (32)$$

\mathcal{I}_j would have positive size only if $M \geq N$. Without loss of generality, we design $(\mathbf{V}_i^J, i = 1, 2, \dots, K)$ such that,

$$\mathbf{H}_{1,1} \mathbf{V}_1^J = \mathbf{H}_{2,1} \mathbf{V}_2^J = \dots = \mathbf{H}_{L_j,1} \mathbf{V}_{L_j}^J = \mathcal{I}_j \quad (33)$$

While the system of equations in ((33)) has more variables than the number of equations, (32) ensures that the system has a unique solution as \mathcal{I}_j lies in the spans of $(\mathbf{H}_{i,1}; i = 1, 2, \dots, K)$.

Let

$$\mathbf{H}_{i,1} = \begin{bmatrix} \mathbf{H}_{i,1}' \\ \mathbf{H}_{i,1}'' \end{bmatrix} \mathcal{I} = \begin{bmatrix} \mathcal{I}_j' \\ \mathcal{I}_j'' \end{bmatrix} \quad \forall i = 1, 2, \dots, K, \quad j = 1, 2, \dots, L_j \quad (34)$$

where $\mathbf{H}_{i,1}'$ contains the M rows of $\mathbf{H}_{i,1}$ and $\mathbf{H}_{i,1}''$ contains the other $N - M$ rows, and \mathcal{I}_j' contains the M rows of \mathcal{I} and \mathcal{I}_j'' contains the other $N - M$ rows. Therefore, we can choose the following design which satisfies (33)

$$\mathbf{V}_i^J = (\mathbf{H}_{i,1}')^{-1} \mathcal{I}_j' \quad \forall i = 1, 2, \dots, K, \quad j = 1, 2, \dots, L_j \quad (35)$$

For the legitimate receiver to remove the jamming signal and decode the legitimate message, it zero forces the jamming signal using the post-processing matrix \mathbf{U} . For the case N_E is odd, each transmitter will align its jamming signal into an $\lfloor \frac{N_E}{2} \rfloor$ -dimensional half space using linear alignment. The remaining 1dimensional space will be equally shared between the two transmitters' jamming signal using real interference alignment [7], yielding each transmitter's jamming signal to occupy $\frac{N_E}{2}$.

The jamming alignment is possible for group j the size of intersection of j is greater than zero or

$$L_j(M - N) + M \geq 0 \quad (36)$$

where the number of jamming streams J_j that can be sent

by each group is constrained to

$$J_j \leq L_j(L_j(M - N) + M) \quad (37)$$

where the J_j streams wastes $\frac{J_j}{L_j}$ dimensions at the receiver for jamming. For maximizing the achievable SDoF, the group with the smaller ratio $\frac{J_j}{L_j}$ is used for jamming first.

The alignment process begins with assigning the maximum number of jamming streams to the largest possible group as it can align the largest number of jamming streams per one dimension wasted at the receiver.

$$D_s \leq \min(KM - NE, N - \frac{N_E}{L}), \quad (38)$$

where L is the result of the following optimization,

$$\text{maximize } L \quad (39)$$

$$\text{subject to, } \frac{M}{N - M} \leq L \leq K \quad (40)$$

$$N_E \leq L(M - N + M) \quad (41)$$

The previous scheme meets the upperbound in 8 at $((L = K \text{ or } \frac{M}{N-M} \leq K) \text{ and } N_E \leq K(K(M-N)+M)) \text{ and at } (KM - N_E < N - \frac{N_E}{N_E}) \text{ achieving } D_s = \min(KM - N_E, N - \frac{N_E}{N_E})$.

C. Achievability for $N + \frac{N_E}{K} > M > N$

In this region the transmitters uses both the aligned and Nullspace jamming methods, each transmitter sends $M - N$ jamming streams using Nullspace jamming and sends $\frac{N_E}{K} - (M - N)$ jamming streams using aligned jamming.

The achievable SDoF is then

$$D_s \leq N - \frac{N_E - K(M - N)}{L} \quad (42)$$

$$D_s \leq N - \frac{N_E - K(M - N)}{L} \quad (43)$$

where L is defined as in (39), and the achievable region meets the upperbound at $(L = K \text{ and } N_E \leq K((K+1)(M - N) + M)) \text{ and at } (K(2M - N) - N_E < N - \frac{N_E}{N_E})$.

$$D_s \leq N - \frac{N_E - K(M - N)}{K} \quad (44)$$

$$\leq M - \frac{N_E}{K} \quad (45)$$

IV. THE TWO USER $M \times M$ INTERFERENCE CHANNEL

Theorem 2. *The number of SDoF of the two user $M \times M$ interference channel is upperbound as,*

$$d_1 + d_2 \leq M - \frac{N_E}{2} \quad (46)$$

Proof: Let d_e^1 and d_e^2 be the maximum degrees of freedom that the eavesdropper can decode out of the transmitters one and two signals, respectively. Suppose that we added $M - N$ antennas to receiver one, this can only improve the coding scheme rate. As receiver one fully receive the signal sent by transmitter two to receiver two X_2 with modified noise, and X_1 can be decoded by receiver one with no interference

by definition. Then d_1 and X_2 occupies two distinct spaces at receiver one, the SDoF is upperbounded then as

$$d_1 + \max(d_e^1, d_2 + d_e^2) \leq M \quad (47)$$

and for both results of $\max(d_e^1, d_2 + d_e^2)$, the following is true

$$d_1 + d_2 + d_e^2 \leq M \quad (48)$$

Similarly, by adding $M - N$ antennas to receiver two, we have

$$d_2 + d_1 + d_e^1 \leq M \quad (49)$$

Moreover, since the eavesdropper has N_E antennas then

$$d_e^1 + d_e^2 = N_E \quad (50)$$

Combining (13), (49), (50)

$$d_1 + d_2 \leq M - \frac{N_E}{2} \quad (51)$$

Theorem 3. *For the two user $M \times M$ interference channel, the following number of SDoF is achievable*

$$d_1 + d_2 \leq M - \frac{N_E}{2} \quad (52)$$

Proof:

For this channel, the jamming is aligned using basic interference alignment method combined with a stochastic encoder similar to the one used in the MAC,

$$\mathbf{H}_{21} \mathbf{V}_1^J = \mathbf{H}_{22} \mathbf{V}_2^J \quad (53)$$

$$\mathbf{H}_{11} \mathbf{V}_1^J = \mathbf{H}_{12} \mathbf{V}_2^J \quad (54)$$

Using this method N_E jamming streams are aligned at $\frac{N_E}{2}$ dimensions at each receiver. This leaves $N - \frac{N_E}{2}$ dimensions free of Jamming at each receiver. As both receivers fully receives both messages and for each receiver to decode its own message the interfering message should occupy an orthogonal space, then

$$d_1 + d_2 \leq M - \frac{N_E}{2} \quad (55)$$

V. CONCLUSION

We studied the K -user MAC channel and the two user interference channel with multiple antennas at the transmitters, legitimate receivers and eavesdroppers. Generalizing new upperbound was established and a new achievable scheme was provided. We showed that our scheme is optimal for the interference channel and partially optimal for the MAC.

REFERENCES

- [1] A. D. Wyner. *The wiretap channel*. Bell systems technical journal, vol. 8, Oct. 1975.
- [2] E. Ekrem and S. Ulukus. *Secrecy in cooperative relay broadcast channels*. IEEE International Symposium on Information Theory, 2008. ISIT 2008.
- [3] Jianwei Xie and S. Ulukus. *Secure Degrees of Freedom of the Gaussian Multiple Access Wiretap Channel*. IEEE International Symposium on Information Theory Proceedings (ISIT), Jul. 2013.
- [4] Frederique Oggier and Babak Hassibi. *The Secrecy Capacity of the MIMO Wiretap Channel*. IEEE Transactions on Information Theory, Vol.57, Aug. 2011

- [5] E. Tekin and A. Yener. *Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy*. In 44th Annual Allerton Conference on Communication, Control and Computing, September 2006.
- [6] E. Ekrem and S. Ulukus. *The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel*. IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 2083–114, Apr. 2011.
- [7] Jianwei Xie and Sennur Ulukus. *Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming*. The Annual Conference on Information Sciences and Systems (CISS), March 2013.
- [8] Ghadamali Bagherikaram, Abolfazl S. Motahari, Amir K. Khandani. *On the Secure Degrees-of-Freedom of the Multiple-Access-Channel*. IEEE Transaction Information Theory, submitted March 2010. Also available at [arXiv:1003.0729]
- [9] Rouheng liu, Wade Trappe. *Securing Wireless communications at the physical layer*. Springer US, 2010.
- [10] Mohamed Amir, Tamer Khattab, Tarek Elfouly. *On the Secure Degrees of freedom of the K-user MAC and 2-user Interference channels*, DOI: 10.13140/RG.2.1.3661.7365.